UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

SHANELL DEAN, JACKIE DE LEON-WALLIN, and ALLISON STORCHEVOY individually and on behalf of all others similarly situated,	:	25-CV-01051 (JAV)
Plaintiffs,	:	
-v-	:	
NEW YORK BLOOD CENTER, INC., and MEMORIAL BLOOD CENTERS,	:	
Defendants.	:	

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Shanell Dean, Jackie De Leon-Wallin, and Allison Storchevoy bring this Consolidated Class Action Complaint ("Complaint") against Defendants New York Blood Center, Inc., and ("NYBC") and Memorial Blood Centers ("MBC") (together with NYBC, "Defendants") individually, on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This Consolidated Class Action arises from a recent cyberattack that resulted in a data breach of sensitive information in the possession and custody and/or control of Defendants (the "Data Breach"). Defendant NYBC is one of the county's largest nonprofit blood collection

and distribution organizations in the United States. MBC, a blood center operating in Minnesota and Wisconsin, merged with NYBC in 2016 and is a division of NYBC. [1]

2. On information and belief, the Data Breach occurred on January 26, 2025. The Data Breach resulted in unauthorized disclosure, exfiltration, and theft of current and former patients' highly personal information, including their "personally identifying information" or "PII", as well as their "protected health information" or "PHI". Plaintiffs refer to both PII and PHI collectively as "Sensitive Information."

3. Upon information and belief, as of March 28, 2025, Defendants still have not sent out formal breach notices to notify Class Members about the Data Breach.

4. Defendants delayed notice to Class Members even though Plaintiffs and thousands of Class Members had their most sensitive personal information accessed, exfiltrated, and stolen, causing them to suffer ascertainable losses in the form of the loss of the benefit of their bargain and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

5. Defendants' online Breach Notice obfuscated the nature of the breach and the threat it posted—refusing to tell patients how many people were impacted, how the breach happened, what precise information was impacted and why Defendants have not yet formally begun notifying victims that hackers had gained access to highly private Sensitive Information.

6. Defendants' failure to timely detect and report the Data Breach made their patients vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their Sensitive Information.

[1] https://www.mbc.org/about-us/about-mbc/#:~:text=In%202016%2C%20Memorial%20Blood%20Centers,Blood%20Center%20Enterprises%20(NYBCe). (February 6, 2025)

7. Defendants knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII and PHI misuse.

8. In failing to adequately protect Plaintiffs' and the Class's Sensitive Information, failing to adequately notify them about the breach, and by obfuscating the nature of the breach, Defendants violated state and federal law and harmed thousands of their current and former patients.

9. Plaintiffs and members of the proposed Class are victims of Defendants' negligence and inadequate cyber security measures. Specifically, Plaintiffs and members of the proposed Class trusted Defendants with their Sensitive Information. But Defendants betrayed that trust. Defendants failed to properly use up-to-date security practices to prevent the Data Breach.

10. Plaintiffs and Class Members are current and former patients of Defendants and Data Breach victims.

11. Accordingly, Plaintiffs, on behalf of themselves and a class of similarly situated individuals, bring this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendants' possession.

PARTIES

12. Plaintiff Shanell Dean is a natural person and citizen of New York, where she intends to remain.

13. Plaintiff Jackie de Leon-Wallin is a natural person and citizen of Minnesota, where she intends to remain.

14. Plaintiff Allison Storchevoy is a natural person and citizen of New York, where she intends to remain.

15. Defendant New York Blood Center, Inc., is a New York corporation with its principal place of business located at 310 East 67th Street, New York, NY 10065.

16. Defendant Memorial Blood Centers is a Minnesota corporation with its principal place of business 310 East 67th Street, New York, NY 10065 USA.

JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). There are at least 100 putative Class Members, the aggregated claims of the individual Class Members exceed the sum or value of $5,000,000 exclusive of interest and costs, and members of the proposed Class are citizens of states different from Defendants.

18. This Court has personal jurisdiction over Defendants because Defendants are headquartered in New York, regularly conducts business in New York, and has sufficient minimum contacts in New York.

19. Venue is proper in this Court because Defendants' principal office is in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District.

STATEMENT OF FACTS

MBC and NYBC Acquire, Collect, and Store Plaintiffs' and Class Members' Sensitive Information

20. NYBC is one of the country's largest independent blood centers, providing "high quality blood and stem cell products and related medical and consultative services to hospitals and

patients."[2] It boasts a total annual revenue of $565 million.[3] MBC operates as a division of NYBC, having merged with NYBC in 2016.[4]

21. Upon information and belief, to obtain healthcare services, current and former patients of Defendants, including Plaintiffs and Class members, were required to provide sensitive and confidential Private Information, including, but not limited to, their names, dates of birth, phone numbers, emails, government ID, social security numbers, health records, insurance information, and other sensitive information, that would be held by Defendants in their computer systems.

22. In the course of their relationship, patients, including Plaintiffs and Class Members, provided Defendant with their private Sensitive Information. Defendants used that Sensitive Information to facilitate their treatment of Plaintiffs and required Plaintiffs to provide that Sensitive Information to obtain treatment and care.

23. In collecting and maintaining its current and former patients' Sensitive Information, Defendants agreed they would safeguard the data in accordance with state law, and federal law. After all, Plaintiffs and Class Members themselves took reasonable steps to secure their Sensitive Information.

24. Plaintiffs and Class members provided their Sensitive Information to Defendants with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

[2] https://www.nybce.org/ (last visited February 6, 2025).
[3] https://projects.propublica.org/nonprofits/organizations/131949477 (last visited February 6, 2025).
[4] https://www.mbc.org/about-us/about-mbc/#:~:text=In%202016%2C%20Memorial%20Blood%20Centers,Blood%20Center%20Enterprises%20(NYBCe). (last visited February 6, 2025).

25. Indeed, NYCB's Privacy Policy promises that "We use reasonable and appropriate technical and organizational measures to protect your personal information" and NYBC "protects the privacy and any information that identifies or could be used to identify you that relates to your health, your treatment or your health insurance benefits."[5]

26. Despite recognizing its duty to do so, on information and belief, Defendants have failed to implement reasonable cybersecurity safeguards or policies to protect their patients' Sensitive Information or supervised their IT or data security agents and employees to prevent, detect, and stop breaches of its systems. As a result, Defendants leave significant vulnerabilities in their systems for cybercriminals to exploit and gain access to patients' Sensitive Information.

The Data Breach

27. According to the online Breach Notice, NYBC admits that on January 26, 2025, it "identified suspicious activity affecting our IT systems." Following an internal investigation, NYBC discovered that "the suspicious activity [was] a result of a ransomware incident." NYBC further admitted that "All operating divisions have been affected to some extent. Our operating divisions include: Blood Bank of Delmarva; Community Blood Center of Greater Kansas City; Connecticut Blood Center; Memorial Blood Centers; Nebraska Community Blood Bank; New Jersey Blood Services; New York Blood Center; and Rhode Island Blood Center." [6]

28. In other words, Defendants' cyber and data security systems were so completely inadequate that it allowed cybercriminals to obtain files containing a treasure trove of thousands of its patients' highly private Sensitive Information.

[5] See e.g. https://www.nybce.org/wp-content/uploads/2022/11/ny-pol-0005_rev_01_hipaa_privacy_notice-English.pdf

[6] https://www.nybce.org/news/articles/cyber/ (February 6, 2025)

29. Through its inadequate security practices, Defendants exposed Plaintiffs' and the Class's Sensitive Information for theft and sale on the dark web.

30. Despite their duties and alleged commitments to safeguard Sensitive Information, Defendants did not in fact follow industry standard practices in securing patients' Sensitive Information, as evidenced by the Data Breach.

31. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiffs' and the Class's Sensitive Information. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiffs' and the Class's financial accounts.

32. Even with several months' worth of credit monitoring services, the risk of identity theft and unauthorized use of Plaintiffs' and Class Members' Sensitive Information is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

33. On information and belief, Defendants failed to adequately train and supervise their IT and data security agents and employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over their patients' Sensitive Information. Defendants' negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the Sensitive Information.

The Data Breach was a Foreseeable Risk of which Defendants were on Notice.

34. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare and healthcare adjacent industry preceding the date of the breach.

35. In light of recent high profile data breaches at other healthcare and healthcare adjacent companies, Defendants knew or should have known that their electronic records and patients' Sensitive Information would be targeted by cybercriminals.

36. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[7] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[8]

37. Indeed, cyberattacks against the healthcare industry have become increasingly common for over ten years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime." [9]

38. Cyberattacks on medical systems and healthcare and healthcare adjacent companies like Defendants have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are

[7] 2021 Data Breach Annual Report, ITRC, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf (last visited January 10, 2024).
[8] *Id*.
[9] Gordon M. Snow Statement, FBI https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector (last visited January 10, 2024).

attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[10]

39. In fact, many high-profile ransomware attacks have occurred in healthcare and healthcare adjacent companies, with an estimated that nearly half of all ransomware attacks being carried out are on healthcare companies, and with 85% of those attacks being ransomware similar to the one occurring here.[11]

40. Therefore, the increase in such attacks, and the attendant risk of future attacks, was widely known to the public and to anyone in Defendants' industry, including Defendants.

Plaintiff Shanell Dean's Experience

41. Plaintiff Shanell Dean obtained services from NYBC. To obtain these services, she was required to provide her Sensitive Information to Defendants.

42. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff Shanell Dean's Sensitive Information in its system.

43. Plaintiff Shanell Dean is very careful about sharing her Sensitive Information. Plaintiff Shanell Dean stores any documents containing her Sensitive Information in a safe and secure location. Plaintiff Shanell Dean has never knowingly transmitted unencrypted Sensitive Information over the Internet or any other unsecured source.

44. Plaintiff Shanell Dean learned of the Data Breach through an online posting by Defendant[12]. According to the post, Defendant's systems were improperly accessed by unauthorized third parties. Upon information and belief, the Sensitive Information Plaintiff

[10] Secret Service Warn of Targeted, Law360, https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited January 10, 2024).
[11] Ransomware explained, CSO, https://www.csoonline.com/article/563507/what-is-ransomware-how-it-works-and-how-to-remove-it.html (last visited January 10, 2024);
[12] https://www.nybce.org/news/articles/cyber/ (last visited Mar. 28, 2025)

Shanell Dean provided to Defendants, including, but not limited, some combination of her name, date of birth, email, phone number, medical information, treatment information and Social Security number, was compromised.

45. As a result of the Data Breach, Plaintiff Shanell Dean made reasonable efforts to mitigate the impact of the Data Breach, including checking her bills and accounts to make sure they were correct. Plaintiff Shanell Dean has spent significant time dealing with the Data Breach, valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

46. Plaintiff Shanell Dean suffered actual injury from having her Sensitive Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her Sensitive Information; (iii) lost or diminished value of Sensitive Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) nominal damages; and (ix) the continued and certainly increased risk to her Sensitive Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Sensitive Information.

47. As a result of the Data Breach, Plaintiff Shanell Dean fears for her personal financial security and uncertainty over what medical information was revealed in the Data Breach. She is experiencing feelings of anxiety, sleep disruption, stress, and fear because of the Data Breach and the resulting invasion of her privacy caused by the exposure of her private

medical information. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

48. As a result of the Data Breach, Plaintiff Shanell Dean anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

49. As a result of the Data Breach, Plaintiff Shanell Dean is presently at risk and will continue to be at increased risk of identity theft and fraud for years to come.

50. Plaintiff Shanell Dean has a continuing interest in ensuring that her Sensitive Information, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Allison Storchevoy's Experience

51. Upon information and belief, Defendants obtained Plaintiff Allison Storchevoy's Sensitive Information in the course of conducting its regular business operations.

52. Upon information and belief, at the time of the Data Breach, Defendants maintained Plaintiff' Allison Storchevoy's Sensitive Information in its system.

53. Plaintiff Allison Storchevoy is very careful about sharing her Sensitive Information. Plaintiff Allison Storchevoy stores any documents containing her Sensitive Information in a safe and secure location. Plaintiff Allison Storchevoy has never knowingly transmitted unencrypted Sensitive Information over the internet or any other unsecured source. Plaintiff Allison Storchevoy would not have entrusted her Sensitive Information to Defendants had she known of Defendants' lax data security policies.

54. Upon information and belief, Plaintiff Allison Storchevoy's Sensitive Information was targeted, accessed, and acquired in the Data Breach.

55. As a result of the Data Breach, Plaintiff Allison Storchevoy made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach. Plaintiff Allison Storchevoy has spent significant time dealing with the Data Breach—valuable time Plaintiff Allison Storchevoy otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

56. Plaintiff Allison Storchevoy suffered actual injury from having her Sensitive Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her Sensitive Information; (iii) lost or diminished value of Sensitive Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) nominal damages; and (ix) the continued and certainly increased risk to her Sensitive Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Sensitive Information.

57. The Data Breach has caused Plaintiff Allison Storchevoy to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed Plaintiff of key details about the Data Breach's occurrence.

58. As a result of the Data Breach, Plaintiff Allison Storchevoy anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

59. As a result of the Data Breach, Plaintiff Allison Storchevoy is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

60. Plaintiff Allison Storchevoy has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Jackie De Leon-Wallin's Experience

61. Plaintiff Jackie De Leon-Wallin is a current MBC patient. As a condition of treatment with MBC, Plaintiff Jackie De Leon-Wallin provided Defendants with her Sensitive Information. Defendants used that Sensitive Information to facilitate their treatment of Plaintiff Jackie De Leon-Wallin and required Plaintiff Jackie De Leon-Wallin to provide that Sensitive Information to obtain treatment and care.

62. Defendants deprived Plaintiff Jackie De Leon-Wallin of the earliest opportunity to guard herself against the Data Breach's effects by failing to promptly notify her about it.

63. As a result of its inadequate cybersecurity, Defendants exposed Plaintiff Jackie De Leon-Wallin's Sensitive Information for theft by cybercriminals and sale on the dark web.

64. Plaintiff Jackie De Leon-Wallin does not recall ever learning that her Sensitive Information was compromised in a data breach incident, other than the Data Breach at issue in this case.

65. As a result of the online Data Breach notice, Plaintiff Jackie De Leon-Wallin spent time dealing with the consequences of the Data Breach, which includes time spent

verifying the legitimacy of the Notice of Data Breach, self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

66. Plaintiff Jackie De Leon-Wallin has and will spend considerable time and effort monitoring her accounts to protect herself from additional identity theft. Plaintiff Jackie De Leon-Wallin fears for her personal financial security and uncertainty over what Sensitive Information was exposed in the Data Breach.

67. Plaintiff Jackie De Leon-Wallin has and is experiencing feelings of anxiety, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

68. Plaintiff Jackie De Leon-Wallin has suffered actual injury in the form of damages to and diminution in the value of their Sensitive Information—a form of intangible property that Plaintiff Jackie De Leon-Wallin entrusted to Defendant, which was compromised in and as a result of the Data Breach.

69. Plaintiff Jackie De Leon-Wallin suffered actual injury from the exposure of her Sensitive Information—which violates her rights to privacy.

70. Plaintiff Jackie De Leon-Wallin has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Sensitive Information being placed in the hands of unauthorized third parties and possibly criminals.

71. Indeed, shortly after the Breach, Plaintiff Jackie De Leon-Wallin was alerted to a fraudulent charge on her SharePoint Credit Union debit card that she did not recognize and

certainly did not authorize. As a result of this fraudulent charge, Plaintiff Jackie De Leon-Wallin was forced to order a new debit card and update all her recurring charges with the new debit card information.

72. Once an individual's Sensitive Information is for sale and access on the dark web, as Plaintiff's Sensitive Information is here as a result of the Breach, cybercriminals are able to use the stolen and compromised to gather and steal even more information.[13] On information and belief, the fraudulent charge on her bank debit card was made possible as a result of Defendants' Data Breach and the subsequent exposure of Plaintiff's Sensitive information to cybercriminals.

73. Plaintiff Jackie De Leon-Wallin has a continuing interest in ensuring that her Sensitive Information, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiffs and the Proposed Class Face Significant Risk of Continued Identity Theft

74. Plaintiffs and members of the proposed Class have suffered injury from the misuse of their Sensitive Information that can be directly traced to Defendants.

75. As a result of Defendants' failure to prevent the Data Breach, Plaintiffs and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their Sensitive Information is used;

b. The diminution in value of their Sensitive Information;

[13] What do Hackers do with Stolen Information, Aura, https://www.aura.com/learn/what-do-hackers-do-with-stolen-information (last visited January 9, 2024).

c. The compromise and continuing publication of their Sensitive Information;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen Sensitive Information; and

h. The continued risk to their Sensitive Information, which remains in Defendants possession and is subject to further breaches so long as Defendants fails to undertake the appropriate measures to protect the Sensitive Information in its possession.

76. Given the type of targeted attack in this case, the sophisticated criminal activity, the volume of data likely compromised in this Data Breach, and the Sensitive Information believed to be involved in this Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Sensitive Information for identity theft crimes—*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

77. Indeed, Plaintiff Jackie De-Leon was already alerted by her bank of unauthorized charges on her debit card.

78. However, such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Sensitive Information was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

79. Consequently, Plaintiffs and Class members are at an increased risk of fraud and identity theft for many years into the future.

80. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class member. This is a reasonable and necessary cost to monitor and protect Class members from the risk of identity theft resulting from Defendants' Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class members would not need to bear, but for Defendants' failure to safeguard their Sensitive Information.

81. Defendants disclosed the Sensitive Information of Plaintiffs and the Class for criminals to use in the conduct of criminal activity. Specifically, Defendants opened up, disclosed, and exposed the Sensitive Information of Plaintiffs and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen Sensitive Information.

82. Defendants' failure to properly notify Plaintiffs and members of the Class of the Data Breach exacerbated Plaintiffs' and the Class's injury by depriving them of the earliest

ability to take appropriate measures to protect their Sensitive Information and take other necessary steps to mitigate the harm caused by the Data Breach.

The Value of Sensitive Information

83. Stolen Sensitive Information is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII alone can be worth up to $1,000.00 depending on the type of information obtained.

84. The value of Plaintiffs' and the Class's Sensitive Information on the black market is considerable. Stolen Sensitive Information trades on the black market for years, and criminals frequently post stolen Sensitive Information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course. It can take victims years to spot identity theft, giving criminals plenty of time to use that information for cash.

85. One such example of criminals using Sensitive Information for profit is the development of "Fullz" packages.

86. Cyber-criminals can cross-reference two sources of Sensitive Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

87. The development of "Fullz" packages means that stolen Sensitive Information from the Data Breach can easily be used to link and identify it to Plaintiffs and the proposed Class' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Sensitive Information stolen by the cyber-criminals in the Data Breach,

criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs' and the Class's stolen Sensitive Information is being misused, and that such misuse is fairly traceable to the Data Breach.

88. Of course, a stolen Social Security number – which, upon information and belief, were compromised for some Class Members in the Data Breach – can be used to wreak untold havoc upon a victim's personal and financial life. The popular person privacy and credit monitoring service LifeLock by Norton notes "Five Malicious Ways a Thief Can Use Your Social Security Number," including 1) Financial Identity Theft that includes "false applications for loans, credit cards or bank accounts in your name or withdraw money from your accounts, and which can encompass credit card fraud, bank fraud, computer fraud, wire fraud, mail fraud and employment fraud; 2) Government Identity Theft, including tax refund fraud; 3) Criminal Identity Theft, which involves using someone's stolen Social Security number as a "get out of jail free card;" 4) Medical Identity Theft, and 5) Utility Fraud.

89. It is little wonder that courts have dubbed a stolen Social Security number as the "gold standard" for identity theft and fraud. Social Security numbers, which were compromised for some Class Members in the Data Breach, are among the worst kind of Private Information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

90. According to the Social Security Administration, each time an individual's Social Security number is compromised, "the potential for a thief to illegitimately gain access

to bank accounts, credit cards, driving records, tax and employment histories and other private information increases." [14] Moreover, "[b]ecause many organizations still use SSNs as the primary identifier, exposure to identity theft and fraud remains."[15]

91. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiff and some Class Members, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[16]

92. In fact, "[a] stolen Social Security number is one of the leading causes of identity theft and can threaten your financial health."[17] "Someone who has your SSN can use it to impersonate you, obtain credit and open bank accounts, apply for jobs, steal your tax refunds, get medical treatment, and steal your government benefits."[18]

93. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of

---

[14] *See* https://www.ssa.gov/phila/ProtectingSSNs.htm#:~:text=An%20organization's%20collection%20and%20use,and%20other%20private%20information%20increases.

[15] *Id.*

[16] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf

[17] *See* https://www.equifax.com/personal/education/identity-theft/articles/-/learn/social-security-number-identity-theft/

[18] *See* https://www.investopedia.com/terms/s/ssn.asp

misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

94. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[19]

95. For these reasons, some courts have referred to Social Security numbers as the "gold standard" for identity theft. *Portier v. NEO Tech. Sols*., No. 3:17-CV-30111, 2019 WL 7946103, at *12 (D. Mass. Dec. 31, 2019) ("Because Social Security numbers are the gold standard for identity theft, their theft is significant . . . . Access to Social Security numbers causes long-lasting jeopardy because the Social Security Administration does not normally replace Social Security numbers."), report and recommendation adopted, No. 3:17-CV-30111, 2020 WL 877035 (D. Mass. Jan. 30, 2020); *see also McFarlane v. Altice USA, Inc*., 2021 WL 860584, at *4 (citations omitted) (S.D.N.Y. Mar. 8, 2021) (the court noted that Plaintiffs' Social Security numbers are: arguably "the most dangerous type of personal information in the hands of identity thieves" because it is immutable and can be used to "impersonat[e] [the victim] to get medical services, government benefits, ... tax refunds, [and] employment." . . . Unlike a credit card number, which can be changed to eliminate the risk of harm following a data breach, "[a] social security number derives its value in that it is immutable," and when it is stolen it can "forever be wielded to identify [the victim] and target her in fraudulent schemes and identity theft attacks.")

[19] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft

96. Similarly, the California state government warns patients that: "[o]riginally, your Social Security number (SSN) was a way for the government to track your earnings and pay you retirement benefits. But over the years, it has become much more than that. It is the key to a lot of your personal information. With your name and SSN, an identity thief could open new credit and bank accounts, rent an apartment, or even get a job."[20]

97. Theft of PHI is also gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[21]

98. The greater efficiency of electronic health records brings the risk of privacy breaches. These electronic health records contain a lot of sensitive information (*e.g.,* patient data, patient diagnosis, lab results, medications, prescriptions, treatment plans, etc.) that is valuable to cybercriminals. One patient's complete record can be sold for hundreds of dollars on the dark web. As such, PHI/PII is a valuable commodity for which a "cyber black market" exists where criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on several underground internet websites. Unsurprisingly, the pharmaceutical industry is at high risk and is acutely affected by cyberattacks, like the Data Breach here.

99. Between 2005 and 2019, at least 249 million people were affected by healthcare data breaches.[22] Indeed, during 2019 alone, over 41 million healthcare records were exposed,

[20] *See* https://oag.ca.gov/idtheft/facts/your-ssn
[21] *Medical I.D. Theft*, EFraudPrevention https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected. (last visited Nov. 6, 2023).
[22] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133/ (last accessed July 24, 2023).

stolen, or unlawfully disclosed in 505 data breaches.[23] In short, these sorts of data breaches are increasingly common, especially among healthcare systems, which account for 30.03 percent of overall health data breaches, according to cybersecurity firm Tenable.[24]

100. According to account monitoring company LogDog, medical data sells for $50 and up on the Dark Web.[25]

101. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[26]

102. A study by Experian found that the average cost of medical identity theft is "about $20,000" per incident and that most victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive to restore coverage.[27] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third of medical identity theft victims saw their insurance premiums rise, and 40 percent were never able to resolve their identity theft at all.[28]

---

[23] https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/ (last accessed July 24, 2023).
[24] https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-incovid-19-era-breaches/ (last accessed July 24, 2023).
[25] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content (last accessed July 20, 2021)
[26] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/ (last accessed July 24, 2023).
[27] *See* Elinor Mills, "Study: Medical Identity Theft is Costly for Victims," CNET (Mar, 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last accessed July 24, 2023).
[28] *Id.; see also Healthcare Data Breach: What to Know About them and What to Do After One,* EXPERIAN, https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-toknow-about-them-and-what-to-do-after-one/ (last accessed July 24, 2023).

103. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[29]

104. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

105. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

106. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[30]

[29] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html

[30] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf

107. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Sensitive Information.

Defendants failed to adhere to FTC guidelines.

108. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendants, should employ to protect against the unlawful exposure of Sensitive Information.

109. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the sensitive consumer information that it keeps;

b. properly dispose of Sensitive Information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

110. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

111. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for

suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

112. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

113. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' Sensitive Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendants Violated HIPAA

114. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information. [31]

115. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII and PHI is properly maintained.[32]

[31] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, inter alia: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

[32] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

116. The Data Breach itself resulted from a combination of inadequacies showing Defendants' failure to comply with safeguards mandated by HIPAA. Defendants' security failures include, but are not limited to:

a. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

d. Failing to ensure compliance with HIPAA security standards by Defendants in violation of 45 C.F.R. § 164.306(a)(4);

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents

that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

117. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendants failed to comply with safeguards mandated by HIPAA regulations.

Defendants Fail to Comply with Industry Standards

118. As noted above, experts studying cyber security routinely identify entities in possession of PII and PHI as being particularly vulnerable to cyberattacks because of the value of the Sensitive Information which they collect and maintain.

119. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[33]

120. Several best practices have been identified that a minimum should be implemented by employers in possession of PII and PHI, like Defendants, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without

[33] How to Protect Your Networks from RANSOMWARE, at 3, *available at:* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view

a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendants failed to follow these industry best practices, including a failure to implement multi-factor authentication.

121. Other best cybersecurity practices that are standard for employers include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendants failed to follow these cybersecurity best practices, including failure to train staff.

122. Upon information and belief, Defendants failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04).

123. These foregoing frameworks are existing and applicable industry standards for an employer's obligations to provide adequate data security for its patients. Upon information and belief, Defendants failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

CLASS ACTION ALLEGATIONS

124. Plaintiffs bring this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following class:

> All individuals residing in the United States whose Sensitive Information was compromised in the Data Breach.

125. Excluded from the Class is Defendants, their agents, affiliates, parents, subsidiaries, any entity in which Defendants have a controlling interest, any of Defendants' officers or directors, any successors, and any Judge who adjudicates this case, including their staff and immediate family.

126. Plaintiffs reserve the right to amend the class definition.

127. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

a. **Numerosity**. Plaintiffs are representative of the Class, consisting of several thousand members, far too many to join in a single action;

b. **Ascertainability**. Members of the Class are readily identifiable from information in Defendants' possession, custody, and control;

c. **Typicality**. Plaintiffs' claims are typical of class claims as each arises from the same Data Breach, the same alleged violations by Defendants, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiffs will fairly and adequately protect the proposed Class's interests. Her interests do not conflict with the Class's interests, and she has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiffs' and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for the Class. Indeed, it will be necessary to answer the following questions:

i. Whether Defendants have a duty to use reasonable care in safeguarding Plaintiffs' and the Class's Sensitive Information;

ii. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

iii. Whether Defendants were negligent in maintaining, protecting, and securing Sensitive Information;

iv. Whether Defendants breached contract promises to safeguard Plaintiffs' and the Class's Sensitive Information;

v. Whether Defendants took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendants Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiffs' and the Class's injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiffs and the Class are entitled to damages, treble damages, or injunctive relief.

128. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

COUNT I
Negligence
(On Behalf of Plaintiffs and the Class)

129. Plaintiffs repeat and reallege all allegations in paragraphs 1 through 128 as if fully set forth herein.

130. Plaintiffs and members of the Class entrusted their Sensitive Information to Defendants. Defendants owed to Plaintiffs and the Class a duty to exercise reasonable care in handling and using Sensitive Information in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

131. Defendants owed a duty of care to Plaintiffs and members of the Class because it was foreseeable that Defendants' failure to adequately safeguard their Sensitive Information in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that Sensitive Information —just like the Data Breach that ultimately came to pass. Defendants acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and the Class's Sensitive Information by disclosing and providing access to this information to unauthorized third parties and by failing to properly supervise both the way the Sensitive Information was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

132. Defendants owed to Plaintiffs and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their Sensitive Information. Defendants also owed a duty to timely and accurately disclose to Plaintiffs and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary

for Plaintiffs and the Class to take appropriate measures to protect their Sensitive Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

133. Defendants owed these duties to Plaintiffs and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendants knew or should have known would suffer injury-in-fact from Defendants' inadequate security protocols. Defendants actively sought and obtained Plaintiffs' and the Class's Sensitive Information.

134. The risk that unauthorized persons would attempt to gain access to the Sensitive Information and misuse it was foreseeable. Given that Defendants hold vast amounts of Sensitive Information, it was inevitable that unauthorized individuals would attempt to access Defendants' databases containing the Sensitive Information —whether by malware or otherwise.

135. Sensitive Information is highly valuable, and Defendants knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Sensitive Information of Plaintiffs and the Class and the importance of exercising reasonable care in handling it.

136. Defendants breached their duties by failing to exercise reasonable care in supervising its employees, agents, contractors, vendors, and suppliers, and in handling and securing the Sensitive Information of Plaintiffs and the Class which actually and proximately caused the Data Breach and Plaintiffs' and the Class's injury. Defendants further breached their duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs' and members of the Class's injuries-in-fact. As a direct and traceable result of Defendants' negligence and/or negligent supervision, Plaintiffs and the Class have suffered or

will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

137. Defendants' breach of their common-law duties to exercise reasonable care and their failures and negligence actually and proximately caused Plaintiffs and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their Sensitive Information by criminals, improper disclosure of their Sensitive Information, lost benefit of their bargain, lost value of their Sensitive Information, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendants' negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiffs and the Class)

138. Plaintiffs repeat and reallege all allegations in paragraphs 1 through 128 as if fully set forth herein.

139. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendants have a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and the Class's Sensitive Information.

140. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect customers or, in this case, patients' Sensitive Information. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendants' duty to protect Plaintiffs' and the members of the Class's Sensitive Information.

141. Defendants breached their duties to Plaintiffs and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Sensitive Information.

142. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and their patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendants were in a position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach.

143. Defendants' duty to use reasonable security measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

144. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential Sensitive Information.

145. Defendants violated their duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiffs' and the Class's Sensitive Information and not complying with applicable industry standards as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of Sensitive Information Defendants collected and stored and the foreseeable consequences of a data breach, including,

specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

146. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

147. Defendants violated their duty under HIPAA by failing to use reasonable measures to protect their PHI and by not complying with applicable regulations detailed *supra*. Here too, Defendants' conduct was particularly unreasonable given the nature and amount of Sensitive Information Defendants collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

148. But for Defendants' wrongful and negligent breach of the duties owed to Plaintiffs and members of the Class, Plaintiffs and members of the Class would not have been injured.

149. The injury and harm suffered by Plaintiffs and members of the Class were the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that they were failing to meet their duties and that their breach would cause Plaintiffs and members of the Class to suffer the foreseeable harms associated with the exposure of their Sensitive Information.

150. Had Plaintiffs and the Class known that Defendants did not adequately protect their Sensitive Information, Plaintiffs and members of the Class would not have entrusted Defendants with their Sensitive Information.

151. Defendants' various violations and their failure to comply with applicable laws and regulations constitute negligence *per se*.

152. As a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of Sensitive Information; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Sensitive Information, entitling them to damages in an amount to be proven at trial.

153. Additionally, as a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and Class members have suffered and will suffer the continued risks of exposure of their Sensitive Information, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect their Sensitive Information in its continued possession.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

154. Plaintiffs repeat and reallege all allegations in paragraphs 1 through 128 as if fully set forth herein.

155. Plaintiffs and the Class delivered their Sensitive Information to Defendants as part of the process of obtaining treatment and services provided by Defendants.

156. Plaintiffs and Class Members entered into implied contracts with Defendants under which Defendants agreed to safeguard and protect such information and to timely and accurately notify Plaintiffs and Class Members if and when their data had been breached and compromised. Each such contractual relationship imposed on Defendants an implied covenant

of good faith and fair dealing by which Defendants were required to perform their obligations and manage Plaintiffs' and Class Members' data in a manner which comported with the reasonable expectations of privacy and protection attendant to entrusting such data to Defendants.

157. In providing their Sensitive Information, Plaintiffs and Class Members entered into an implied contract with Defendants whereby Defendants, in receiving such data, became obligated to reasonably safeguard Plaintiffs' and the other Class Members' Sensitive Information, including by virtue of representations in their privacy policies.

158. In delivering their Sensitive Information to Defendants, Plaintiffs and Class Members intended and understood that Defendants would adequately safeguard that data.

159. Plaintiffs and the Class Members would not have entrusted their Sensitive Information to Defendants in the absence of such an implied contract.

160. Defendants accepted possession of Plaintiffs' and Class Members' Sensitive Information.

161. Had Defendants disclosed to Plaintiffs and Class Members that Defendants did not have adequate computer systems and security practices to secure patients' Sensitive Information, Plaintiffs and members of the Class would not have provided their Sensitive Information to Defendants.

162. Defendants recognized that patients' Sensitive Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiffs and Class Members.

163. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendants.

164. Defendants breached the implied contract with Plaintiffs and Class Members by failing to take reasonable measures to safeguard the Sensitive Information of Plaintiffs and Class Members, who reasonably believed and expected that Defendants' data security practices complied with relevant laws and regulations (including HIPAA and FTC guidelines on data security) and were consistent with industry standards.

165. Defendants breached the implied contract with Plaintiffs and Class Members by failing to promptly notify them of the access to and exfiltration of their Sensitive Information.

166. As a direct and proximate result of the breach of the contractual duties, Plaintiffs and Class Members have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiffs and the Class Members include: (a) the invasion of privacy; (b) the compromise, disclosure, theft, and unauthorized use of Plaintiffs' and Class Members' Sensitive Information; (c) economic costs associated with the time spent to detect and prevent identity theft, including loss of productivity; (d) monetary costs associated with the detection and prevention of identity theft; (e) economic costs, including time and money, related to incidents of actual identity theft; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their Sensitive Information; (g) the diminution in the value of the services bargained for as Plaintiffs and Class Members were deprived of the data protection and security that Defendants promised when Plaintiffs and the proposed class entrusted Defendants with their Sensitive Information; and (h) the continued and substantial risk to Plaintiffs' and Class Members' Sensitive Information, which remains in the Defendants' possession with inadequate measures to protect Plaintiffs' and Class Members' Sensitive Information.

COUNT IV
Breach of Fiduciary Dury
(On Behalf of Plaintiffs and the Class)

167. Plaintiffs repeat and reallege all allegations in paragraphs 1 through 128 as if fully set forth herein.

168. In light of the special relationship between Defendants and Plaintiffs and Class Members, whereby Defendants became guardian of Plaintiffs' and Class Members' Sensitive Information, Defendants became a fiduciary by their undertaking and guardianship of the Sensitive Information, (1) to act primarily for Plaintiffs and Class Members, (2) for the safeguarding of their Sensitive Information; (3) to timely notify Plaintiffs and Class Members of a Data Breach's occurrence and disclosure; and (4) to maintain complete and accurate records of what information (and where) Defendants did and does store.

169. Defendants have a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of Defendants' relationship with their patients, in particular, to keep secure their Sensitive Information.

170. Defendants have a fiduciary duty to act for the benefit of Plaintiffs and Class Members because of the high degree of trust and confidence inherent to the nature of the relationship between Plaintiffs and Class Members on the one hand and Defendants on the other, including with respect to their Sensitive Information.

171. Defendants breached their fiduciary duties to Plaintiffs and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period of time.

172. Defendants breached their fiduciary duties to Plaintiffs and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiffs' and Class Members' Sensitive Information.

173. Defendants breached their fiduciary duties owed to Plaintiffs and Class Members by failing to timely notify and/or warn Plaintiffs and Class Members of the Data Breach.

174. Defendants breached their fiduciary duties to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' Sensitive Information.

175. As a direct and proximate result of Defendants' breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Sensitive Information; (iii) lost or diminished value of Sensitive Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) nominal damages; and (viii) the continued and certainly increased risk to their Sensitive Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Sensitive Information.

COUNT V
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

176. Plaintiffs repeat and reallege all allegations in paragraphs 1 through 128 as if fully set forth herein.

177. This claim is pleaded in the alternative to the breach of contractual duty claim.

178. Plaintiffs and members of the Class conferred a benefit upon Defendants in providing Sensitive Information to Defendants. In exchange, Plaintiffs and Class Members should have had their Sensitive Information protected with adequate data security.

179. Defendants appreciated or had knowledge of the benefits conferred upon them by Plaintiffs and the Class. Defendants also benefited from the receipt of Plaintiffs' and the Class's Sensitive Information, as this was used to facilitate the treatment, services, and goods they sold to Plaintiffs and the Class.

180. Defendants failed to secure Plaintiffs' and Class Members' Sensitive Information and, therefore, did not fully compensate Plaintiffs or Class Members for the value that their Sensitive Information provided.

181. Defendants acquired the Sensitive Information through inequitable record retention as they failed to investigate and/or disclose the inadequate data security practices previously alleged.

182. If Plaintiffs and Class Members had known that Defendants would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their Sensitive Information, they would have entrusted their Sensitive Information at Defendants or obtained medical services from Defendants.

183. Plaintiffs and Class Members have no adequate remedy at law.

184. Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Sensitive Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendants instead calculated to increase their own profit at the expense of

Plaintiffs and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to their own profit. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendants' decision to prioritize their own profits over the requisite security and the safety of their Sensitive Information.

185. Under principles of equity and good conscience, Defendants should not be permitted to retain the full value of Plaintiffs' and the Class's Sensitive Information because Defendants failed to adequately protect their Sensitive Information. Plaintiffs and the proposed Class would not have provided their Sensitive Information to Defendants had they known Defendants would not adequately protect their Sensitive Information.

186. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiffs and members of the Class all unlawful or inequitable proceeds received by them because of their misconduct and Data Breach.

COUNT VI
Invasion of Privacy—Intrusion Upon Seclusion
(On Behalf of Plaintiffs and the Class)

187. Plaintiffs repeat and reallege all allegations in paragraphs 1 through 128 as if fully set forth herein.

188. Plaintiffs and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential Sensitive Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

189. Defendants owed a duty to their patients, including Plaintiffs and the Class, to keep this information confidential.

190. The unauthorized acquisition (i.e., theft) by a third party of Plaintiffs' and Class Members' Sensitive Information is highly offensive to a reasonable person.

191. The intrusion was into a place or thing which was private and entitled to be private. Plaintiffs and the Class disclosed their sensitive and confidential information to Defendants as part of their obtainment of medical services, but they did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiffs and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

192. The Data Breach constitutes an intentional interference with Plaintiffs' and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

193. Defendants acted with a knowing state of mind when they permitted the Data Breach because they knew their information security practices were inadequate.

194. Defendants acted with a knowing state of mind when they failed to notify Plaintiffs and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

195. Acting with knowledge, Defendants had notice and knew that their inadequate cybersecurity practices would cause injury to Plaintiffs and the Class.

196. As a proximate result of Defendants' acts and omissions, the Sensitive Information of Plaintiffs and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages.

197. Unless and until enjoined and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class

because their Sensitive Information are still maintained by Defendants with their inadequate cybersecurity system and policies.

198. Plaintiffs and the Class have no adequate remedy at law for the injuries relating to Defendants' continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendants' inability to safeguard the Sensitive Information of Plaintiffs and the Class.

199. In addition to injunctive relief, Plaintiffs, on behalf of themselves and the other members of the Class, also seeks compensatory damages for Defendants' invasion of privacy, which includes the value of the privacy interest invaded by Defendants, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

COUNT VII
Violation Of The New York Deceptive Trade Practices Act ("GBL")
New York Gen. Bus. Law § 349
(On Behalf of Plaintiffs and the Class)

200. Plaintiffs repeat and reallege all allegations in paragraphs 1 through 128 as if fully set forth herein.

201. Defendants engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and furnishing of services, in violation of N.Y. Gen. Bus. Law § 349(a), including but not limited to the following:

a. Misrepresenting material facts to Plaintiffs and the Class by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Class Members' Sensitive Information from unauthorized disclosure, release, data breaches, and theft;

b. Misrepresenting material facts to Plaintiffs and the Class by representing that they did and would comply with the requirements of federal and state laws pertaining to the privacy and security of Class Members' Sensitive Information;

c. Omitting, suppressing, and/or concealing material facts of the inadequacy of its privacy and security protections for Class Members' Sensitive Information;

d. engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Class Members' Sensitive Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws; and,

e. engaging in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Data Breach to the Class in a timely and accurate manner, contrary to the duties imposed by N.Y. Gen. Bus. Law § 899-aa(2).

202. Defendants knew or should have known that their network and data security practices were inadequate to safeguard the Class Members' Sensitive Information entrusted to them, and that risk of a data breach or theft was highly likely.

203. Defendants should have disclosed this information because Defendants were in a superior position to know the true facts related to the defective data security.

204. Defendants' failure constitutes false and misleading representations, which have the capacity, tendency, and effect of deceiving or misleading consumers (including Plaintiffs and Class Members) regarding the security of Defendants' network and aggregation of Sensitive Information.

205. The representations upon which consumers (including Plaintiffs and Class Members) relied were material representations (e.g., as to Defendants' adequate protection of

Sensitive Information), and patients (including Plaintiffs and Class Members) relied on those representations to their detriment.

206. Defendants' conduct is unconscionable, deceptive, and unfair, as it is likely to, and did, mislead consumers acting reasonably under the circumstances. As a direct and proximate result of Defendants' conduct, Plaintiffs and other Class Members have been harmed, in that they were not timely notified of the Data Breach, which resulted in profound vulnerability to their personal information and other financial accounts.

207. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard Class Members' Sensitive Information and that the risk of a data security incident was high.

208. Defendants' acts, practices, and omissions were done in the course of Defendants' business of providing medical services to consumers in the State of New York.

209. As a direct and proximate result of Defendants' unconscionable, unfair, and deceptive acts and omissions, Plaintiffs' and Class Members' Sensitive Information was disclosed to third parties without authorization, causing and will continue to cause Plaintiffs and Class Members damages.

210. Plaintiffs and Class Members were injured because:

a. Plaintiffs and Class Members would not have accepted Defendants services had they known the true nature and character of Defendants' data security practices;

b. Plaintiffs and Class Members would not have entrusted their Sensitive Information to Defendants in the absence of promises that Defendants would keep their information reasonably secure, and

c. Plaintiffs and Class Members would not have entrusted their Sensitive Information to Defendants in the absence of the promise to monitor their computer systems and networks to ensure that they adopted reasonable data security measures.

211. Defendants' multiple, separate violations of GBL §349 were the direct and proximate cause of Plaintiffs' and Class Members' injuries (as detailed *supra*).

212. As a result, Plaintiffs and the Class Members have been damaged in an amount to be proven at trial.

213. Plaintiffs bring this action on behalf of themselves and Class Members for the relief requested above and for the public benefit to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiffs, Class Members and the public from Defendants' unfair, deceptive, and unlawful practices. Defendants' wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

214. Plaintiffs and Class Members seek relief under N.Y. Gen. Bus. Law § 349(h), including, but not limited to, actual damages, treble damages, statutory damages, injunctive relief, and/or attorney's fees and costs.

215. On behalf of themselves and other members of the Class, Plaintiffs seek to enjoin the unlawful acts and practices described herein, to recover their actual damages or fifty dollars, whichever is greater, three times actual damages, and reasonable attorneys' fees.

216. Also as a direct result of Defendants' violation of GBL § 349, Plaintiffs and the Class Members are entitled to damages as well as injunctive relief, including, but not limited to, ordering Defendants to: (i) strengthen their data security systems and monitoring

procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

PRAYER FOR RELIEF

Plaintiffs and the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiffs as class representatives, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiffs and the Class;

D. Enjoining Defendants from further deceptive practices and making untrue statements about the Data Breach and the stolen Sensitive Information;

E. Awarding Plaintiffs and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiffs and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

Dated: March 31, 2025

Respectfully submitted,

By: */s/Andrew J. Shamis*

Andrew J. Shamis
New York Bar No. 5195185
Leanna A. Loginov
New York Bar No. 5894753
SHAMIS & GENTILE, P.A.
14 NE First Avenue, Suite 705
Miami, Florida 33132
Telephone: 305-479-2299
ashamis@shamisgentile.com
lloginov@shamisgentile.com

Samuel J. Strauss (*Pro Hac Vice* forthcoming)
Raina Borelli (*Pro Hac Vice* forthcoming)
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
(872) 263-1100
(872) 263-1109 (facsimile)
sam@straussborrelli.com
raina@straussborrelli.com

Vicki J. Maniatis, Esq.
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
405 East 50th Street
New York, New York 10022
Phone: (212) 594-5300
vmaniatis@milberg.com

David K. Lietz (*Pro Hac Vice forthcoming)*
MILBERG COLEMAN BRYSON

PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Avenue NW, Suite 440
Washington, D.C. 20015-2052
Telephone: (866) 252-0878
Facsimile: (202) 686-2877
dlietz@milberg.com

Attorneys for Plaintiffs and Proposed Class